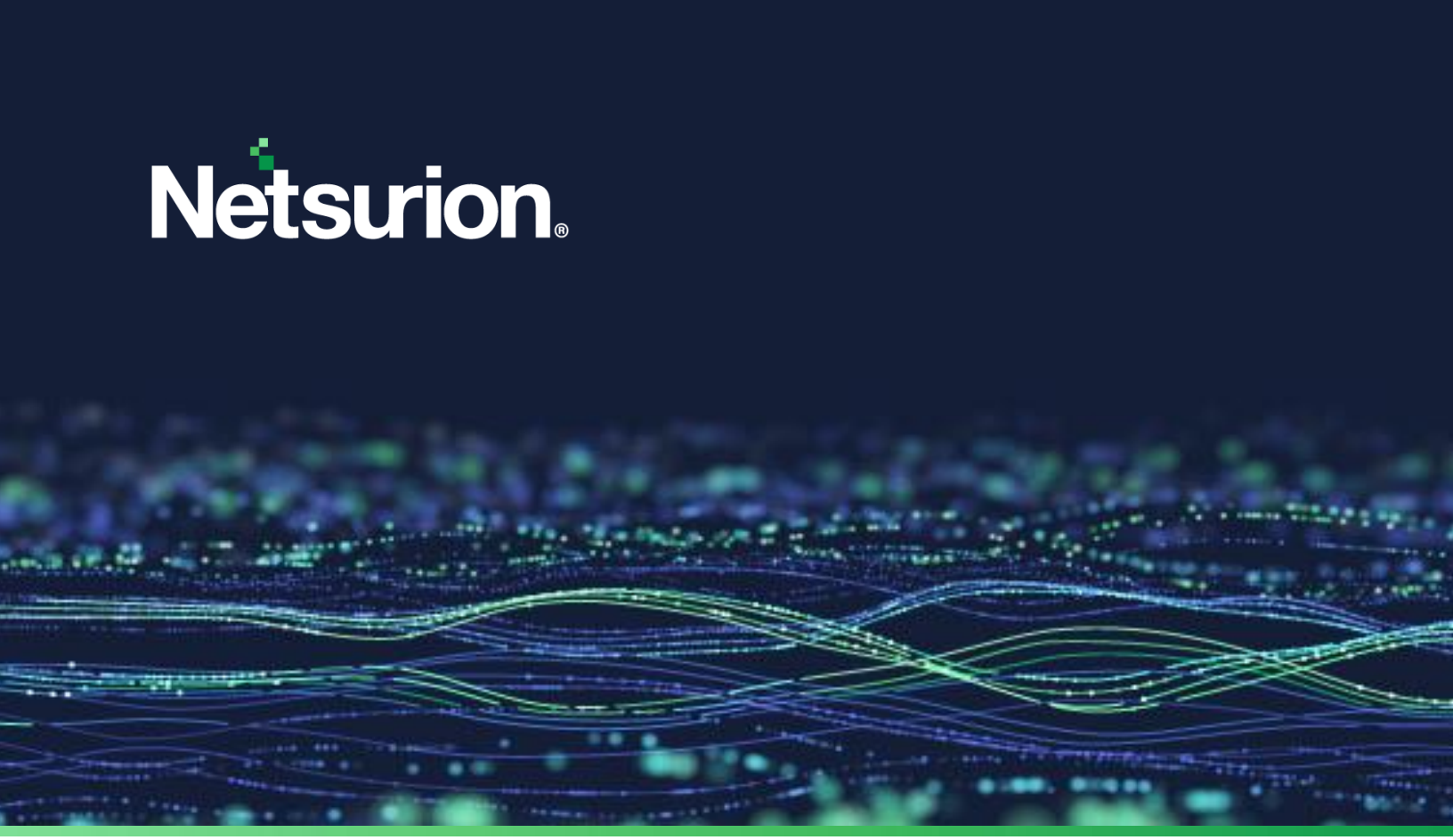


How-To Guide

Integrate Kemp LoadMaster with Netsurion Open XDR

Publication Date

September 22, 2023

Abstract

This guide provides instructions to configure and integrate Kemp LoadMaster with Netsurion Open XDR to retrieve its logs via syslog integration and forward them to Netsurion Open XDR.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Kemp LoadMaster v7.2.56.x to v7.2.59.x, and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Kemp LoadMaster in Netsurion Open XDR.

Table of Contents

1 Overview

Kemp LoadMaster is a load balancing and application delivery software built on a bespoke Linux operating system. It optimizes web infrastructure in terms of high availability, performance, scalability, ease of management, and security.

Netsurion Open XDR manages logs retrieved from Kemp LoadMaster. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Kemp LoadMaster.

2 Prerequisites

- Admin privileges to access the Kemp LoadMaster web console.
- Port **514** (TCP) must be opened and dedicated for syslog communication only.
- Must have the **Web Application Firewall (WAF)** service enabled on respective Kemp LoadMaster device.

Note:

If the **Web Application Firewall (WAF)** service is not enabled, then the following DSI assets will not reflect any data.

- **Dashboard:** Kemp LoadMaster - WAF events.
- **Report:** Kemp LoadMaster - WAF events.
- **Saved Searches:** Kemp LoadMaster - WAF events.

- The Data Source Integration package.

Note

To get the Data Source Integration package, contact your Netsurion Account Manager.

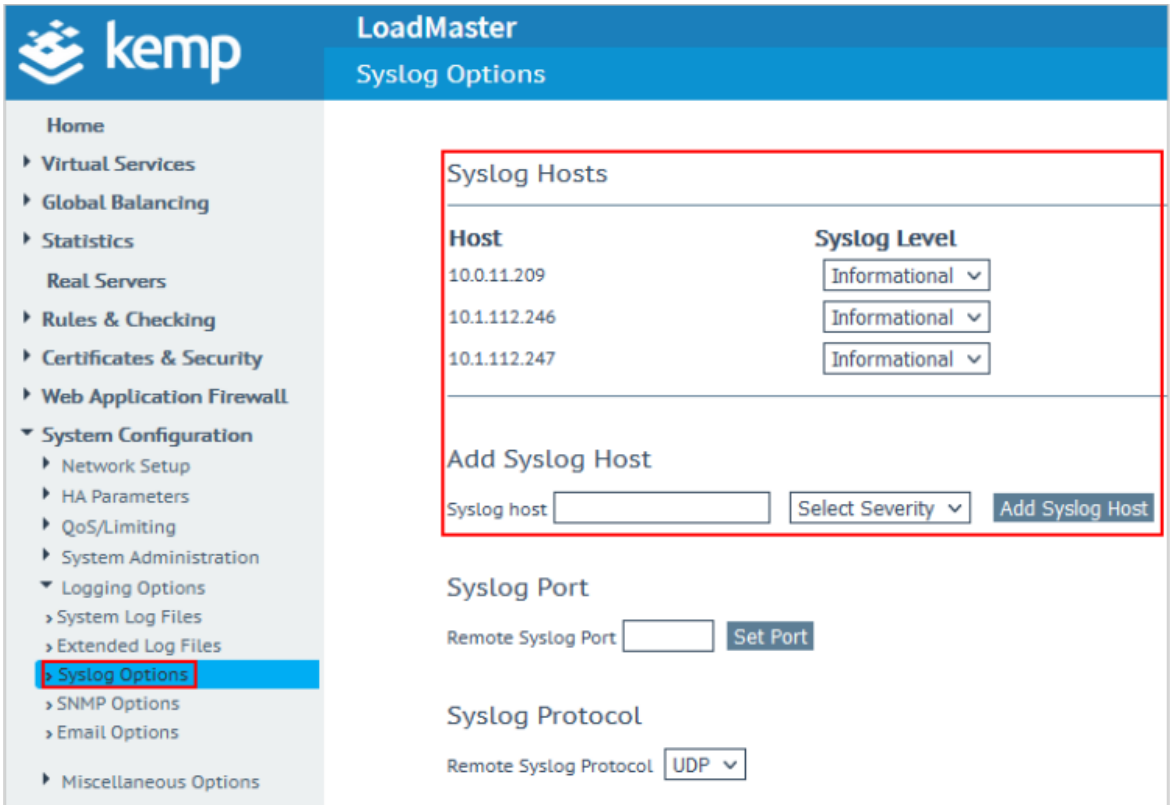
3 Integrating Kemp LoadMaster with Netsurion Open XDR

Integrate Kemp LoadMaster to Netsurion Open XDR via syslog with the help of the syslog feature available in the LoadMaster Web Console.

3.1 Configuring the Syslog Settings

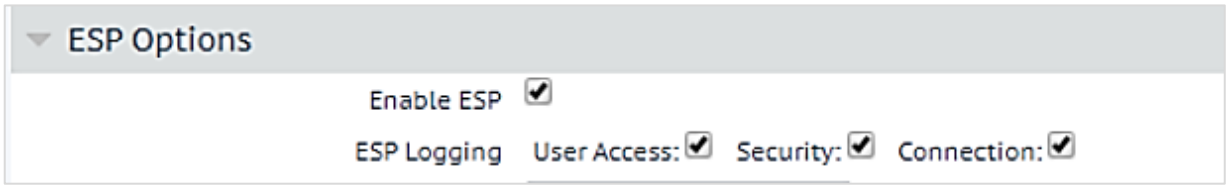
Perform the following procedure to configure the syslog setting in in LoadMaster Web Console.

1. Log in to the **LoadMaster** web console and navigate to **System Configuration** > **Logging Options** > **Syslog Options**.
2. In the **Syslog Options** interface, provide the specified details in each section.



   a. In **Add Syslog Host**, provide the details for Syslog host and select the severity level, and then click **Add Syslog Host** to add the specified host details.
      - **Syslog host:** Specify the Netsurion Open XDR FQDN/ IP address (recommended **FQDN**).
      - **Severity:** Select **Informational** from the drop-down list.
   b. In **Syslog Port**, for **Remote Syslog Port**, specify the port number (**514**) and click **Set Port** to set the port information.
   c. In **Syslog Protocol**, for **Remote Syslog Protocol**, select **UDP/TCP/TLS** (recommended using **TCP**) syslog protocol from the drop-down list.

3. In the **LoadMaster** web console, navigate to **Virtual Services** > **View/Modify Services** and go to the relevant Virtual Service(s), click **Modify** and expand the **ESP Options** section, and then select all the **ESP Options** check boxes to enable and capture the ESP logs.



Note:

ESP Options must be in enabled state for the relevant virtual services.

4. In the **LoadMaster** web console, navigate to **System Configuration** > **Logging Options** > **Extended Log Files** and select the **Disable Local Extended ESP Logs** check box to enable forwarding the ESP logs to Netsurion Open XDR.

   When this **Disable Local Extended Logs** is in enabled state, the logs will be sent directly to the remote logger (the defined syslog host) instead of storing locally.

Note:

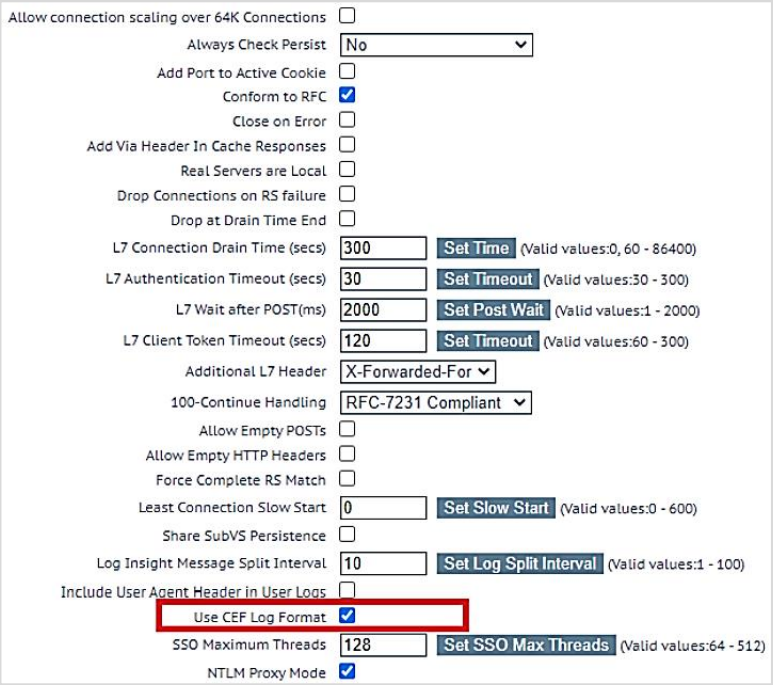
If the **Disable Local Extended Logs** is in disabled state (which is the default option), the ESP (Edge Security Pack) logs will be written to the local storage of the LoadMaster and will not be sent to any remote syslog servers. If no remote logger is defined and the **Disable Local Extended Logs** is in enabled state, then no logs will be recorded on LoadMaster local storage as well.

3.2 Enabling the CEF Format

In the **LoadMaster** web console, go to **System Configuration** > **Miscellaneous Options** > **L7 Configuration** and click **Use CEF log format** check box to enable the CEF log format.

Note:

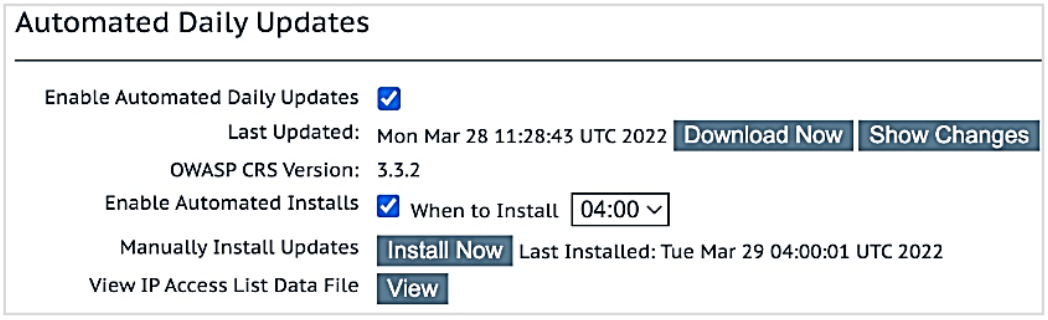
Enabling the CEF log format changes only the ESP logs format from default to CEF format.



3.3 Verifying the Web Application Firewall Service Status

Perform the following procedure to verify the Web Application Firewall service status on Kemp LoadMaster web console.

1. Log in to the **LoadMaster** web console with admin privileges and go to **Web Application Firewall** > **Access settings**.
2. In the **Access** settings, verify if **Automated Daily Updates** section is enabled to confirm the status of the WAF service.



4 Data Source Integration (DSI) in Netsurion Open XDR

After the logs are received by Netsurion Open XDR, configure the Data Source Integrations in Netsurion Open XDR.

The Data Source Integrations package contains the following files for Kemp LoadMaster.

- Categories_Kemp LoadMaster.iscat
- Alerts_Kemp LoadMaster.isalt
- Reports_Kemp LoadMaster.etcrx
- KO_Kemp LoadMaster.etko
- Dashboards_Kemp LoadMaster.etwd
- Templates_Kemp LoadMaster.ettd

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in Netsurion Open XDR.

4.1 Alerts

Name	Description
Kemp LoadMaster: Attempted XSS attack detected	Generated whenever the Kemp LoadMaster device detects potentially malicious content that may be linked to XSS (cross-site scripting).

4.2 Reports

Name	Description
Kemp LoadMaster - ESP events	Provides details on events related to Edge Security Pack (ESP) detected by Kemp LoadMaster.
Kemp LoadMaster - WAF events	Provides details on events related to Web Application Firewall (WAF) detected by Kemp LoadMaster.

4.3 Dashboards

Name	Description
Kemp LoadMaster - Security events	Displays all the security related events.
Kemp LoadMaster - Connection events	Displays all the connection related events.
Kemp LoadMaster - SSOMGR events	Displays all the Single Sign-On (SSO) related events.
Kemp LoadMaster - WAF events	Displays all the Web Application Firewall (WAF) events.
Kemp LoadMaster - User related events	Displays all the user triggered events.

4.4 Saved Searches

Name	Description
Kemp LoadMaster - ESP events	Provides details on events related to Edge Security Pack (ESP) detected by Kemp LoadMaster.
Kemp LoadMaster - WAF events	Provides details on events related to Web Application Firewall (WAF) detected by Kemp LoadMaster.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support